Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
05/01/2024	1	Elaboração do processo de gestão de riscos de segurança da informação.

1. INTRODUÇÃO

O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis (BRASIL, 2021). Este processo envolve a identificação, avaliação e mitigação de ameaças e vulnerabilidades que possam afetar a confidencialidade, integridade e disponibilidade dos dados e sistemas de uma organização.

No Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO) a gestão de riscos de segurança da informação é responsável por identificar, avaliar, tratar, monitorar, controlar e documentar riscos relacionados à segurança dos ativos de informação, podendo ser um serviço, recurso ou sistema de informação (ABNT, 2019). Sua finalidade é evitar o desperdício de recursos públicos e potencializar a efetividade dos processos organizacionais, garantindo a implementação de ações preventivas sempre que necessário para proteger as informações sensíveis e os sistemas contra ameaças e vulnerabilidades.

Dentro do contexto apresentado, este documento tem como objetivo estabelecer as características do processo de gestão de riscos de segurança da informação utilizado pelo Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO). Ele está estruturado em uma breve introdução, definições, gestão de riscos de segurança da informação, papéis e responsabilidades, matriz RACI, indicador de desempenho, processos relacionados, práticas recomendadas e referências.

1.1. Escopo

O escopo do processo de gestão de riscos de segurança da informação abrange uma série de atividades destinadas a identificar, avaliar, mitigar e monitorar os riscos de segurança que uma organização enfrenta em relação aos seus ativos de informação. Ele envolve:

a) identificação de ativos e avaliação de riscos: identificar e classificar os ativos de informação (dados, sistemas, *hardware e software*) relevantes para o IFTO. Em seguida, avaliar as ameaças potenciais e vulnerabilidades que podem afetar esses ativos;

b) análise de ameaças e vulnerabilidades: analisar as possíveis ameaças que podem explorar as vulnerabilidades nos sistemas de informação da organização. Isso pode incluir ameaças internas, externas, naturais e tecnológicas;

c) avaliação de impacto: avaliar o impacto potencial que uma ameaça pode ter sobre os ativos de informação. Isso envolve compreender as consequências financeiras, operacionais e de reputação associadas a diferentes tipos de incidentes de segurança;

d) identificação de controles de segurança: identificar e implementar controles de segurança para mitigar ou reduzir os riscos identificados. Isso pode incluir controles técnicos (*firewalls*, criptografia), controles administrativos (políticas, treinamento) e controles físicos (restrições de acesso físico);

e) análise de riscos residuais: após a implementação dos controles de segurança, realizar uma análise adicional para determinar os riscos residuais, ou seja, os riscos que permanecem após a aplicação dos controles;

f) planejamento de resposta a incidentes: desenvolver planos de resposta a incidentes para lidar com possíveis violações de segurança, incluindo ações a serem tomadas em caso de incidentes de segurança;

g) monitoramento e revisão contínuos: implementar um processo contínuo de monitoramento e revisão dos riscos de segurança para identificar novas ameaças, mudanças nos ativos de informação e atualizações necessárias nos controles de segurança; e

h) conscientização e treinamento: promover a conscientização sobre segurança da informação entre os funcionários e fornecer treinamentos regulares para garantir a compreensão e o cumprimento das políticas de segurança.

1.2. Objetivos

O objetivo geral deste processo é resguardar as informações contra ameaças e vulnerabilidades, assegurando a continuidade dos negócios por meio da identificação, avaliação e tratamento de riscos que podem impactar a segurança dos dados e informações do IFTO. Para alcançar esse objetivo, foram estabelecidos os seguintes objetivos específicos:

a) identificação de riscos: identificar e compreender os riscos de segurança da informação que podem afetar os ativos da organização, incluindo dados, sistemas, redes e processos;

b) avaliação de riscos: avaliar a probabilidade e o impacto dos riscos identificados, considerando as ameaças potenciais e as vulnerabilidades existentes nos sistemas de informação;

c) priorização de riscos: priorizar os riscos de segurança da informação

com base na probabilidade de ocorrência e no impacto potencial, para direcionar recursos de mitigação para as áreas mais críticas;

d) mitigação e controle: implementar controles e medidas de segurança adequadas para reduzir, mitigar ou eliminar os riscos identificados, incluindo controles técnicos, procedimentais e organizacionais;

e) resposta a incidentes: desenvolver planos e procedimentos de resposta a incidentes para lidar eficazmente com incidentes de segurança quando ocorrerem, minimizando danos e tempo de inatividade;

f) conformidade e governança: garantir conformidade com regulamentações, normas e requisitos legais relacionados à segurança da informação, mantendo uma boa governança de segurança;

g) gestão de custos: gerenciar eficientemente os recursos financeiros, humanos e tecnológicos para implementar medidas de segurança proporcionalmente aos riscos identificados;

h) melhoria contínua: Estabelecer um processo contínuo de revisão e aprimoramento dos controles de segurança da informação, levando em consideração a evolução das ameaças e tecnologias;

i) conscientização e treinamento: educar e treinar os servidores para aumentar a conscientização sobre práticas de segurança da informação e promover uma cultura de segurança na organização; e

j) proteção da reputação e continuidade dos negócios: proteger a reputação da organização, evitando violações de dados e garantindo a continuidade das operações, mesmo em face de incidentes de segurança.

1.3. **Abrangência**

A gestão de riscos de segurança da informação possui uma abrangência ampla e engloba diversos aspectos da organização. Essa abrangência abarca:

a) ativos de informação: envolve a identificação e avaliação de todos os ativos de informação críticos para a organização, como dados, sistemas, redes, hardware, software, instalações físicas e recursos humanos envolvidos;

b) ameaças e vulnerabilidades: considera ameaças internas e externas que possam comprometer a segurança da informação, incluindo *malware*, ataques cibernéticos, falhas de segurança, desastres naturais, falhas humanas, entre outros;

c) âmbito operacional: compreende diferentes áreas da organização, incluindo TI, operações, recursos humanos, jurídico, financeiro, *compliance* e outras unidades que lidam com dados sensíveis;

d) processos e procedimentos: analisa os processos existentes e os procedimentos de segurança implementados para mitigar riscos. Isso inclui a revisão de políticas de segurança, acesso a dados, procedimentos de backup, entre outros;

e) conformidade: considera requisitos regulatórios e normativos aplicáveis ao IFTO, garantindo conformidade com leis de proteção de dados e políticas internas.

f) controles e medidas de segurança: inclui a implementação de controles técnicos, procedimentais e organizacionais para mitigar riscos, como *firewalls*, criptografia, políticas de segurança, gestão de acesso, entre outros.

g) gestão de incidentes: engloba planos de resposta a incidentes, que são parte integrante da gestão de riscos, ajudando a minimizar o impacto e a restaurar a normalidade após um evento de segurança;

h) análise contínua: envolve uma revisão regular e contínua dos riscos de segurança, considerando a evolução das ameaças, mudanças na infraestrutura e novos requisitos regulatórios para manter a eficácia das medidas de segurança;

i) conscientização, educação e treinamento: educação e treinamento contínuos dos usuários para garantir que estejam cientes das políticas de segurança, entendam as ameaças atuais e saibam como agir para proteger os dados; e

j) cultura organizacional: inclui a promoção de uma cultura de segurança da informação, onde a importância da segurança é reconhecida em todos os níveis da organização.

1.4. **Benefícios esperados**

Com a execução deste processo espera-se alcançar os seguintes benefícios:

a) proteção de ativos de informação: identifica e protege os ativos críticos de informação da organização contra ameaças internas e externas, ajudando a evitar violações de dados, perda de informações e danos à reputação;

b) redução de riscos: permite a identificação proativa, avaliação e mitigação de riscos de segurança, reduzindo a probabilidade de incidentes e minimizando o impacto caso ocorram;

c) conformidade: ajuda a garantir conformidade com regulamentações e normas de segurança, evitando multas e sanções legais decorrentes de não conformidade com leis de proteção de dados;

d) economia de recursos: ajuda a alocar recursos de forma mais eficiente, concentrando-se nos riscos mais críticos e direcionando investimentos para áreas que necessitam de mais proteção;

e) resiliência operacional: melhora a resiliência da organização, garantindo a continuidade dos negócios mesmo diante de ameaças ou incidentes de segurança, minimizando o tempo de inatividade;

f) tomada de decisão informada: fornece informações precisas sobre riscos de segurança, permitindo que a liderança tome decisões informadas sobre investimentos em segurança e estratégias para mitigar riscos;

g) melhoria da reputação: ao evitar violações de dados e incidentes de segurança, a organização preserva sua reputação e a confiança dos

clientes, parceiros e partes interessadas;

h) gestão de custos: ajuda a reduzir custos associados a incidentes de segurança, como custos de recuperação, compensações por danos e perda de negócios;

i) consciência de segurança: promove uma cultura de segurança dentro da organização, aumentando a conscientização entre os funcionários sobre práticas seguras e comportamentos responsáveis em relação à segurança da informação; e

j) adaptação às mudanças: permite uma adaptação ágil a mudanças nas ameaças de segurança, tecnologias emergentes e novos regulamentos, mantendo a organização resiliente e atualizada.

2. DEFINIÇÕES

Para fins de compreensão dos termos utilizados neste processo serão utilizados os seguintes conceitos e definições, conforme detalham as normas 31000 (ABNT, 2018) e 27005 (ABNT, 2019):

a) ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através de exploração de vulnerabilidades;

b) análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

c) avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

d) ativos da informação: meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

e) consequência/impacto: resultado de um evento que afeta os objetivos;

f) comunicação do risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

g) controle: medida que mantém e/ou modifica o risco;

h) estimativa de riscos: processo utilizado para atribuir valores à probabilidade e consequências de um risco;

i) evento: ocorrência ou mudança em um conjunto específico de circunstâncias;

j) gestão de riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos;

k) incerteza: estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade;

l) identificação de riscos: processo para localizar, listar e caracterizar elementos do risco;

m) mapa de gerenciamento de riscos: documento que relaciona os riscos identificados, sua origem, natureza e tipo;

n) matriz de riscos: ferramenta de gerenciamento de riscos que permite de forma visual identificar quais são os riscos que devem receber mais atenção. Tabela que apresenta duas dimensões: probabilidade e impacto que permite classificar os riscos através da avaliação do impacto versus a probabilidade;

o) matriz de probabilidade x impacto: documento que especifica combinações de probabilidade de ocorrência de um risco e do impacto causado por sua ocorrência, permitindo assim calcular o nível de risco a partir da multiplicação dos valores atribuídos à probabilidade e ao impacto;

p) plano de gestão de riscos: plano que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos. Os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades. O plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização;

q) plano de tratamento de riscos: plano que descreve as ações de tratamento do risco, identificando os responsáveis, com o objetivo de reduzir o risco a um nível aceitável (risco residual);

r) probabilidade: chance de algo acontecer;

s) risco: efeito da incerteza nos objetivos. Possibilidade de evento que afeta negativamente a realização dos objetivos da instituição e seus processos. Pode ser positivo, negativo ou ambos, e pode abordar, criar e resultar em oportunidades e ameaças. Risco é um evento hipotético, cuja ocorrência pode afetar de forma positiva ou negativa uma organização. Ele possui chance de ocorrência futura que não é nula e apresenta impacto ou oportunidade significante;

t) risco de segurança da informação: possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização;

u) segurança da informação: preservação da confidencialidade, integridade disponibilidade da informação. Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

v) tratamento de riscos: fase da gestão de riscos que envolve a decisão entre reter, evitar, transferir (compartilhar) ou reduzir os riscos;

x) TI: Tecnologia da Informação; e

w) vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

3. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Conforme destacado por Brasil (2013), a gestão de riscos de segurança da informação é o conjunto de processos que permitem

identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. Este processo objetiva minimizar a ocorrência de ameaças que podem interferir (negativamente) no recurso de informação utilizado pela instituição para atingir os seus objetivos corporativos. No IFTO este processo é composto por 6 (seis) fases, conforme demonstra a figura 1.

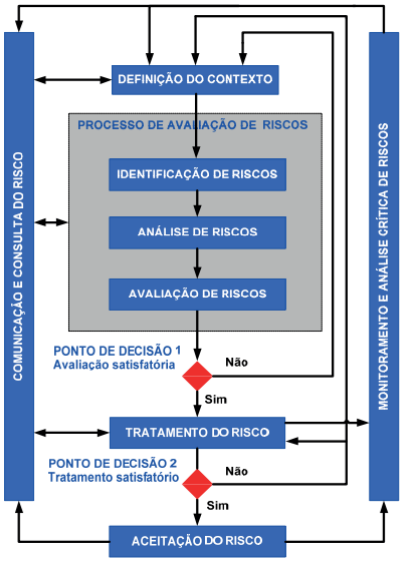

Figura 1 - Processo de gestão de riscos de segurança da informação (ABNT, 2019)

Conforme mostra a figura 1, o processo de gestão de riscos de segurança da informação utiliza como referência a norma ABNT/ISO/IEC 27005 (ABNT, 2019). O processo é composto pelas fases: definição do contexto, processo de avaliação de riscos (identificação de riscos, análise de riscos e avaliação de riscos), tratamento do risco, aceitação do risco, monitoramento e análise crítica de riscos, e comunicação e consulta do risco.

No IFTO este processo é estabelecido com vistas a minimizar possíveis impactos associados aos ativos, possibilitando a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança da informação, a fim de adequar riscos aos níveis aceitáveis para o IFTO.

Ele é executado de forma iterativa e incremental o que permite minimizar o tempo e o esforço despendidos na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados. A tabela 1 apresenta a entrada, fases e saída deste processo.

Tabela 1 - Processo de gestão de riscos de segurança da informação

Processo de gestão de riscos de segurança da informação	
Entrada	Inventário de riscos de segurança da informação.
Fases	1. Definição do contexto. 2. Processo de avaliação de riscos (identificação, análise e avaliação de riscos). 3. Tratamento do risco. 4. Aceitação do risco. 5. Comunicação e consulta do risco. 6. Monitoramento e análise crítica de riscos.
Saídas	Mapa de gerenciamento de riscos. Plano de tratamento de riscos.

3.1. **Definição do contexto**

Esta fase envolve a compreensão do ambiente externo e interno no qual o objeto de gestão de riscos se encontra inserido. Além disso, busca identificar parâmetros e critérios a serem considerados no processo de gestão de riscos (TCU, 2020; Brasil, 2021). Nesta fase é realizada análise da estrutura organizacional, responsabilidades, processos, sistemas de informação e relações com os demais setores da instituição. No contexto, o escopo é definido, levando em consideração o conjunto de controles definidos nas políticas e normas publicadas.

Nesta fase são definidos os critérios básicos do processo como por exemplo: a abordagem da gestão de riscos (políticas e procedimentos, implementação dos controles selecionados e monitoramento); avaliação de riscos (criticidade dos ativos de informação envolvidos, prioridades para o tratamento do riscos etc); impacto (nível de classificação do ativo de informação afetado, ocorrências de violação da segurança da informação, operações comprometidas, perda de oportunidades de negócio e de valor financeiro, interrupção de planos e não cumprimento de prazos e danos a reputação); aceitação do risco (nível desejado de risco, risco estimado, tratamento adicional futuro) (ABNT, 2019).

Segundo a norma ABNT 27005 (ABNT, 2019) na definição do contexto também são definidos o escopo e limites da gestão de riscos de segurança da informação de forma a assegurar que todos os ativos relevantes sejam considerados no processo de avaliação de riscos. Entende-se como contexto interno e externo o conjunto de eventos que possam influenciar a capacidade da organização de atingir seus objetivos estratégicos (BRASIL, 2021). Além disso, os limites precisam ser identificados para permitir o reconhecimento dos riscos que possam transpor esses limites.

Ao definir o escopo e os limites deve-se considerar as seguintes informações: objetivos estratégicos, políticas e estratégias da organização, processos de negócio, funções e estrutura da organização, política de segurança da informação da organização, a abordagem da organização à gestão de riscos, ativos de informação, localidades em que a organização se encontra e suas características geográficas, restrições que afetam a organização, expectativas das partes interessadas, ambiente sociocultural, interfaces. Deve-se fornecer justificativa para exclusões do escopo.

Portanto na definição do contexto a instituição deve definir o processo adequado para a gestão de riscos de segurança da informação, identificar e analisar as partes interessadas neste processo, definir papéis e responsabilidades para organizar o processo. Deve-se também definir as alçadas para a tomada de decisões e estabelecer a especificação dos registros a serem mantidos. Esta fase possui as seguintes atividades:

a) identificar quais objetivos ou resultados devem ser alcançados;

b) identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados;

c) identificar as pessoas envolvidas nesses processos e especialistas na área;

d) mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, *stakeholders* etc.);

e) definir os objetos de gestão de risco mais importantes para a sua unidade ou trabalho; e

f) definir os objetivos/resultados de cada objeto.

Dentro do contexto apresentado, a organização deve definir o seu sistema de gestão de riscos de segurança da informação baseado no contexto definido. A figura 2 apresenta o modelo utilizado pelo IFTO.

Figura 2 - Sistema de Gestão de Riscos de Segurança da Informação (FERNANDES, 2011)

3.2. **Processo de avaliação de riscos**

O processo de avaliação de riscos tem como objetivo quantificar ou descrever o risco qualitativamente, capacitando os gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos. Esta fase determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes (ou que possam existir), identifica os controles existentes e seus efeitos no risco identificado, determina as consequências possíveis e, finalmente, prioriza os riscos derivados e os ordena de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto (ABNT, 2019). A avaliação de riscos é composta pelas atividades: identificação, análise e avaliação de riscos que serão detalhadas nos próximos subitens.

3.2.1. **Identificação de riscos**

Segundo a norma 27005 (ABNT, 2019) o propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer. Esta atividade deve incluir riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente. Esta atividade é composta pelas tarefas:

a) identificação dos ativos de informação que precisam ser protegidos: identificar os ativos e seus responsáveis dentro do escopo onde serão desenvolvidas as ações de segurança da informação e comunicações;

b) identificação das ameaças: define a lista de ameaças com a identificação do tipo e da fonte das ameaças;

c) identificação dos controles existentes: define a lista de todos os controles existentes e planejados, sua implementação e a situação de utilização;

d) identificação das vulnerabilidades dos ativos: lista de vulnerabilidades associadas aos ativos, ameaças e controles; e

e) identificação das consequências: identificar os impactos que perdas de disponibilidade, integridade, confidencialidade e autenticidade podem causar nestes ativos.

Ao efetuar o mapeamento e avaliação dos riscos deve ser considerado as tipologias de riscos recomendadas na instrução normativa conjunta nº 1 (Brasil, 2016) e CGU (2021).

a) **riscos operacionais:** eventos que podem comprometer as atividades da instituição, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

b) **riscos de imagem/reputação do órgão:** eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade da instituição em cumprir sua missão institucional;

c) **riscos legais:** eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade; e

d) **riscos financeiros/orçamentários:** eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Para a identificação das causas do risco é importante uma análise das diversas fontes de riscos existentes no processo, tais como:

a) **processo:** decorrente de diretrizes estratégicas e da formalização/modelagem de processos, incluídos os métodos, procedimentos e regulamentações de planejamento, execução, controle e monitoramento. Os mecanismos de comunicação e repositório de conhecimento também se enquadram nesta fonte;
b) **pessoas:** decorrente de operações humanas, onde são requeridas condutas apropriadas, competências, conhecimentos e habilidades;
c) **externa:** decorrente do ambiente externo à organização como desastres naturais, conjuntura político-econômica, imprevisibilidade de fornecedores;
d) i**nfraestrutura:** decorrente dos recursos de infraestrutura física ou lógica (sistemas de TI) da organização; e
e) **recursos humanos ou financeiros:** decorrente da disponibilidade de recursos humanos ou financeiros.

Após a identificação dos riscos, causas e consequências, é necessário identificar quais controles estão presentes no processo e mitigam os riscos identificados. A tabela 2 apresenta os tipos de controle com o nível de maturidade e probabilidade de ocorrência do risco. Esta escala é uma adaptação do PMBOK publicada por PMI (2017).

Tabela 2 – Escala de tipos de controle de risco

Tipo de Controle	Nível de Maturidade	Probabilidade de ocorrer o risco
Corretivo	Inexistente	Elevada
	Fraco	Muito Alta
Detectivo	Insatisfatório	Alta
Preventivo	Satisfatório	Média
	Forte	Baixa

Fonte: PMI (2021)

Conforme apresenta a tabela 3 os tipos de controle são classificados em: corretivo, detectivo e preventivo.

a) **corretivo:** apresenta medidas que podem ser executadas quando um risco já foi causado;

b) **detectivo:** visa à identificação de um erro ou irregularidade depois que este tenha ocorrido; e

c) **preventivo:** controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência.

3.2.2. **Análise de riscos**

Esta atividade refere-se ao desenvolvimento da compreensão sobre o risco e à determinação do nível de impacto. Ela é responsável por compreender, criticar e estimar o nível de criticidade de cada risco, determinado com base na probabilidade (chance de ocorrer) e no impacto (consequências) sobre um ou mais objetivos do processo. Para a análise de riscos deve-se realizar minimamente as tarefas:

a) identificar os impactos para a missão do órgão ou entidade que podem resultar de falhas de segurança, levando em consideração as consequências de uma perda de disponibilidade, integridade, confidencialidade ou autenticidade destes ativos;

b) identificar a probabilidade real de ocorrência de falhas de segurança, considerando as vulnerabilidades prevalecentes, os impactos associados a estes ativos e as ações de segurança da informação e comunicações atualmente implementadas na instituição;

c) estimar os níveis de riscos; e

d) determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos pela instituição.

A análise de riscos é realizada de forma quantitativa e qualitativa.

a) **análise quantitativa de riscos:** efetua a análise numérica do efeito dos riscos identificados; e

b) **análise qualitativa de riscos:** avalia a exposição ao risco priorizando os riscos que serão objetos de análise ou ação adicional. A análise qualitativa dos riscos é feita a partir da definição de escalas de probabilidade e impacto através da técnica de matriz de probabilidade e impacto.

As escalas de risco podem variar de acordo com o objeto de gestão e com o grau de precisão na definição dos níveis de probabilidade. As escalas de probabilidade e impacto do risco, seguem as recomendações da metodologia de gestão de riscos CGU (Brasil, 2021). A tabela 3 apresenta as escalas de probabilidade de ocorrência do risco definidos pela instituição.

Tabela 3 - Escala de probabilidade de ocorrência do risco

Probabilidade	Descrição	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	3

Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá. As circunstâncias indicam claramente essa possibilidade.	5

Fonte: Controladoria Geral da União (Brasil, 2021).

Conforme apresenta a tabela 4 a escala de probabilidade do risco é definida de forma quantitativa de acordo com o peso definido.

O cálculo do impacto consiste no resultado da materialização de um dado risco, medido por critérios preferencialmente quantitativos. A avaliação da relevância do impacto dos riscos é realizada através da relevância do impacto em cada área (imagem, financeiro, legislação e operacional) conferindo uma nota ao impacto. Essa nota poderá se abrandar ou agravar de acordo com o nível de tolerância (tempo) à ação saneadora.

O IFTO define uma escala adaptada do referencial básico de gestão de riscos do TCU (2018b) para realizar o cálculo do nível de impacto em razão de que o impacto varia de acordo com a área impactada. Quando um risco impactar mais de uma área, será considerada a área mais impactada. A tabela 4 apresenta a definição dos pesos adotados para cálculo de impacto de riscos.

Tabela 4 - Escala de impacto do risco

Impacto	Descrição	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação /divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos.	2
Médio	Moderado impacto nos objetivos, porém, recuperável.	3
Alto	Significativo impacto nos objetivos, de difícil reversão.	4
Muito alto	Catastrófico impacto nos objetivos, de forma irreversível.	5

Fonte: Controladoria Geral da União (Brasil, 2021)

O nível de risco processual é definido através da multiplicação entre os valores de probabilidade e impacto, ou seja, o provável impacto nos objetivos do processo organizacional. A partir do resultado do cálculo, o risco pode ser classificado dentro das faixas definidas na tabela 5.

Tabela 5 - Classificação de riscos

Classificação	Faixa
Baixo - RB	0 – 4,99
Médio - RM	5 – 11,99
Alto - RA	12 – 19,99
Extremo - RE	20 – 25

Fonte: Controladoria Geral da União (Brasil, 2021)

Os possíveis resultados da combinação das escalas de probabilidade e impacto são apresentados na tabela 6.

Tabela 6 - Matriz de Riscos

Matriz de riscos						
Impacto	Muito alto (5)	5 RM	10 RM	15 RA	20 RE	25 RE
	Alto (4)	4 RB	8 RM	12 RA	16 RA	20 RE
	Médio (3)	3 RB	6 RM	9 RM	12 RA	15 RA
	Baixo (2)	2 RB	4 RB	6 RM	8 RM	10 RM
	Muito Baixo (1)	1 RB	2 RB	3 RB	4 RB	5 RM
		Muito Baixa (1)	Baixa 2	Média 3	Alta 4	Muito alta 5
		Probabilidade				

Fonte: Controladoria Geral da União (Brasil, 2021)

3.2.3. **Avaliação de riscos**

Esta atividade envolve a comparação do limite de exposição a riscos, a fim de determinar se o risco é aceitável ou não e as medidas de segurança necessárias para mitigar esses riscos. A avaliação de riscos compara os resultados da análise de riscos com os critérios de riscos estabelecidos para determinar onde é necessária ação adicional. Nesta atividade os objetivos a serem alcançados são: a definição de quais controles serão empregados para reduzir alguns destes riscos, a retenção ou aceitação de outros riscos, a ação de evitar outros riscos, a transferência de alguns desses riscos a outros agentes, e a definição de um plano de tratamento do risco.

Os riscos são avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos é realizada por meio de análises qualitativas. O limite de exposição a riscos representa o nível de risco acima do qual é desejável o tratamento do risco. Os riscos são avaliados quanto à sua condição de inerentes e residuais (Brasil, 2021).

a) **inerentes:** processo em questão sem nenhum mecanismo de controle implementado;

b) **residual:** processo em questão com os atuais mecanismos de controle implementados.

A avaliação de riscos gera uma lista de riscos priorizados de acordo com os critérios de avaliação de riscos definidos em relação aos cenários de incidentes que podem levar a esses riscos.

3.3. **Tratamento do risco**

Esta fase compreende o planejamento e a realização de ações para modificar o nível de risco por meio da implementação de medidas de

segurança. O nível de risco pode ser modificado por meio de medidas de resposta ao risco que mitiguem, transfiram ou evitem esses riscos. Para isso, são definidas estratégias: evitar, transferir, aceitar ou mitigar. Estas estratégias estão detalhadas na tabela 7.

A escolha da estratégia de tratamento dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco. Para cada possibilidade de tratamento detectada em função do risco identificado, devem ser observados, no que couber a eficácia das ações de segurança da informação, as restrições técnicas, as restrições físicas estruturais, as restrições operacionais, as restrições organizacionais, os requisitos legais e a relação custo-benefício (BRASIL, 2021).

O resultado desta atividade é o plano de tratamento de riscos. Esta fase envolve as seguintes atividades:

a) **planejar as respostas aos riscos:** no planejamento de resposta a riscos deverão ser desenvolvidas opções e ações para aumentar as oportunidades e reduzir as ameaças relacionadas aos objetivos estratégicos de TI. Para definir as estratégias de respostas são adotadas as recomendações do PMBOK (PMI, 2017).

b) **estratégias para respostas aos riscos negativos ou ameaças:** para tratar os riscos negativos ou ameaças são utilizadas as estratégias: evitar ou eliminar, transferir, mitigar e aceitar, conforme mostra a tabela 7. Estas estratégias são adaptadas de CGU (2018).

Tabela 7 - Estratégia para riscos negativos ou ameaças

Estratégia	Descrição
Evitar/Eliminar (Alto)	Um risco normalmente é evitado quando é classificado como "alto" ou "extremo", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Evitar o risco significa encerrar o processo organizacional (CGU, 2018).
Transferir (Muito Alto)	Transfere um risco para terceiro, transferindo os impactos e a responsabilidade. Passa a responsabilidade e impactos do risco para uma terceira parte, geralmente na forma de subcontratação. Um risco transferido não é eliminado, este ainda poderá se materializar e, por isso, deve ser monitorado.
Mitigar (Médio)	Um risco normalmente é mitigado quando é classificado como "alto" ou "extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de identificação e análise de riscos (CGU, 2018).
Aceitar (Baixo)	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco (CGU, 2018).

Fonte: Controladoria Geral da União (2018)

A tabela 8 apresenta as estratégias utilizadas pelo IFTO para mitigar os riscos negativos ou ameaças para a área de segurança da informação. A partir desta definição são definidos os controles a serem aplicados.

c) **estratégias para respostas aos riscos positivos ou oportunidades:** para tratar os riscos positivos ou oportunidades deverão ser utilizadas as estratégias: explorar, compartilhar, melhorar e aceitar. A tabela 8 apresenta as estratégias definidas para a área de segurança da informação.

Tabela 8 - Estratégia para riscos positivos ou oportunidades

Estratégia	Descrição
Explorar	Muda-se a estratégia para garantir que a oportunidade seja aproveitada. Garante que a oportunidade ocorra para explorar seus benefícios. Procura eliminar a incerteza associada ao risco positivo, adicionando trabalho ou mudando o projeto para assegurar que a oportunidade ocorra.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo (CGU, 2018).
Melhorar	Aumenta a probabilidade e/ou impacto de uma oportunidade. São tomadas ações proativas para que as chances (probabilidade) ou o impacto positivo sejam aumentados. Identificar os principais causadores desses riscos positivos ajuda a aumentar a probabilidade de ocorrência.
Aceitar	A aceitação do risco envolve a criação de planos de contingências para serem implementados se os riscos ocorrerem.

Fonte: Diretoria de Planejamento e Desenvolvimento Institucional CGU (2018).

A tabela 9 apresenta as estratégias utilizadas pelo IFTO para mitigar os riscos positivos ou oportunidades para a área de segurança da informação. A partir desta definição são definidos os controles a serem aplicados.

d) **níveis de confiança dos controles:** deverão ser definidos os controles para a gestão de riscos de acordo com o nível de confiança existente. Recomenda-se o uso da escala definida pela Controladoria-Geral da União (CGU, 2018) e pelo Tribunal de Contas da União (TCU, 2018c). A tabela 9 apresenta os níveis de confiança dos controles adotados para a segurança da informação.

Tabela 9 - Níveis de confiança dos controles

Controle	Descrição
Inexistente	Nenhum nível de confiança. Controles inexistentes, mal desenhados ou mal implementados.
Fraco	Nível de confiança de 20%. Controles têm abordagens ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.

Mediano	Nível de confiança de 40%. Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.
Satisfatório	Nível de confiança de 60%. Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
Forte	Nível de confiança de 80%. Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.

Fonte: Tribunal de Contas da União (2018c)

O artefato principal desta fase é o plano de tratamento dos riscos. Este documento deve conter minimamente: descrição do risco, ação de tratamento, responsável, prazo e monitoramento.

3.4. **Aceitação do risco**

Esta fase deve assegurar que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Isto é especialmente importante em uma situação em que a implementação de controles é omitida ou adiada, por exemplo, devido aos custos (ABNT, 2019).

3.5. **Monitoramento e análise crítica de riscos**

Fase responsável por assegurar que o contexto, o resultado do processo de avaliação de riscos e do tratamento do risco, assim como os planos de gestão, permaneçam relevantes e adequados às circunstâncias. Esta fase compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos, os planos de tratamento de riscos, os controles e outros assuntos de interesse.

Esta fase tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da instituição, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos. Envolve a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras. Considera o tempo necessário para que as medidas mitigadoras produzam seus efeitos.

Esta fase é parte integrante do processo de gestão e de tomada de decisão e acompanha o ciclo de planejamento institucional. A atividade possui as seguintes atividades: estabelecer indicadores de acompanhamento e controle de riscos, acompanhar a evolução dos riscos, divulgar o acompanhamento do controle de riscos e gerar relatórios de monitoramento do controle de riscos.

As atividades de controle de riscos de segurança da informação são realizadas através de procedimentos estabelecidos e executados para mitigar os riscos definidos para o tratamento dos riscos. Elas são executadas através de controles internos de gestão preventivos e detectivos, através do plano de tratamento de riscos, juntamente com listas de verificação.

O plano de gestão de riscos de segurança da informação deve ser acompanhado sistematicamente em reuniões de planejamento. Durante as reuniões são avaliadas as modificações dos atributos de situação, probabilidade de ocorrência e impacto dos riscos, bem como os valores para os gatilhos e a efetividade do plano de resposta para cada um dos riscos inventariados.

3.6. **Comunicação e consulta do risco**

Esta fase objetiva alcançar um consenso sobre como gerenciar os riscos por meio da troca e/ou compartilhamento das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, impacto, tratamento e aceitabilidade dos riscos.

A fase refere-se à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos sobre determinado objeto, observada a classificação da informação quanto ao sigilo. Esta fase fornece as informações relativas ao risco e ao seu tratamento para todos aqueles processos que possam influenciar ou ser influenciados por esse risco, sob pena de ele se materializar plenamente.

4. **PAPÉIS E RESPONSABILIDADES**

Um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e atribuídas a uma pessoa, equipe ou função. Para realizar a gestão de riscos em segurança da informação são definidos papéis e responsabilidades para cada ator envolvido no processo. Para cada risco mapeado e avaliado é associado um agente responsável formalmente identificado.

4.1. Alta Administração

Representa o mais alto nível estratégico e decisório de um órgão ou entidade, seja ela parte da Administração Pública Federal Direta ou Indireta. Compete ao representante deste nível as seguintes responsabilidades:

a) prover a orientação e o apoio necessário às ações de gestão de riscos de segurança da informação, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes;

b) disponibilizar os recursos (humanos, tecnológicos e financeiros) para a execução da política e processo de gestão de riscos de segurança da informação no âmbito do IFTO.

4.2. Comitê de Segurança da Informação

Grupo de pessoas que representam áreas finalísticas do IFTO. Compete a este grupo de pessoas as seguintes responsabilidades:

a) avaliar e aprovar política, processo e plano para gestão de riscos de

segurança da informação; e

b) propor melhorias para a política e processo de gestão de riscos de segurança da informação.

4.3. Gestor de Segurança da Informação

Servidor(a) designado para gerir a segurança da informação. Compete à esta pessoa as seguintes responsabilidades:

a) propor a política e processo de gestão de riscos de segurança da informação;

b) coordenar o processo de gestão de riscos de segurança da informação;

c) designar agente responsável pela gestão de riscos de segurança da informação, dentre os servidores efetivos do IFTO;

d) aprovar o plano de gestão de riscos de segurança da informação;

e) aprovar o relatório de identificação, análise e avaliação dos riscos de segurança da informação e encaminhá-lo à alta administração;

f) aprovar o relatório de tratamento de riscos de segurança da informação; e

g) propor medidas preventivas à alta administração.

4.4. Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Grupo de pessoas composto por servidores públicos civis ocupantes de cargo efetivo, com capacitação técnica compatível com as atividades dessa equipe. Compete à estas pessoas a seguinte responsabilidade:

a) avaliar política, norma, processo, plano, procedimentos e controles sobre gestão de riscos de segurança da informação.

4.5. Setor de TI (Diretoria de Tecnologia da Informação e setores de TI das unidades do IFTO)

Agente responsável pela gestão de riscos de segurança da informação. Compete ao setor as seguintes responsabilidades:

a) identificar os riscos relacionados à segurança da informação;

b) definir o contexto da análise de riscos, definindo os critérios da análise de riscos, a matriz de riscos (Probabilidade x Impacto) e os níveis de risco aceitáveis relevantes para o contexto em análise;

c) associar um agente responsável para cada risco mapeado e avaliado, formalmente identificado para resposta aos riscos;

d) assegurar que o risco seja gerenciado de acordo com as diretrizes estabelecidas neste documento;

e) garantir que as informações adequadas sobre o risco estejam disponíveis e atualizadas;

f) gerenciar e reportar informações adequadas sobre o gerenciamento de riscos;

g) informar o gestor de riscos qualquer dificuldade durante a implementação das ações de tratamento de riscos;

h) elaborar e executar o plano de gestão de riscos de segurança da informação;

i) elaborar o o relatório de identificação, análise e avaliação dos riscos de segurança da informação;

j) elaborar o relatório de tratamento de riscos de segurança da informação; e

k) informar o gestor de segurança da informação sobre o surgimento de novos riscos a partir da implementação das ações de tratamento.

4.6. Usuários

Pessoas que utilizam os dados e informações processados pelo IFTO. Compete aos usuários as seguintes responsabilidades:

a) utilizar os dados e informações no IFTO prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade; e

b) notificar os riscos relacionados à segurança da informação.

5. MATRIZ RACI

A matriz RACI apresentada na tabela 10 é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: *responsible, accountable, consulted e informed.*

a) ***responsible (responsável):*** pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo;

b) ***accountable (responsabilizado):*** dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um *Accountable*;

c) ***consulted (consultado):*** pessoas que deverão ser consultadas durante a execução da atividade; as informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade; e

d) ***informed (informado):*** pessoas que serão informadas acerca do progresso da execução da atividade.

Tabela 10 - Matriz de responsabilidades

Fase	AA	CSI	GSI	ETIR	STI	U

Definição do contexto	A	C/I	C/I	R	C/I	I
Identificação de riscos	A	C/I	C/I	C	R	I
Análise de riscos	A	C/I	C/I	C	R	I
Avaliação de riscos	A	C/I	C/I	C	R	I
Tratamento do risco	A	C/I	C/I	C	R	I
Aceitação do risco	A	C/I	C/I	R	C	I
Monitoramento e análise crítica de riscos	A	C/I	R	C	C	I
Comunicação e consulta do risco	A	C/I	C/I	C	R	I

Fonte: Diretoria de Tecnologia da Informação

Legenda:

AA: Alta Administração.

CSI: Comitê de Segurança da Informação.

GSI: Gestor Institucional de Segurança da Informação.

ETIR: Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

STI: Setor de Tecnologia da Informação (Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO).

U: Usuário

6. INDICADOR DE DESEMPENHO

O processo de gestão de riscos de segurança da informação será monitorado e constantemente medido através de indicador de desempenho. Esse indicador tem como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. A tabela 11 apresenta o indicador de desempenho do processo.

Tabela 11 - Indicador de desempenho

Indicador	Quantidade de riscos de segurança da informação gerenciados.
Descrição	Quantificar riscos identificados e gerenciados durante o ano.
Objetivo	Calcular a quantidade de riscos de segurança da informação gerenciados durante o ano.
Periodicidade	Anual.
Fonte	Plano de Tratamento de Riscos de Segurança da Informação
Fórmula	Total de riscos gerenciados durante o ano.
Meta	Gerenciar riscos de segurança da informação.

Fonte: Diretoria de Tecnologia da Informação

7. PROCESSOS RELACIONADOS

Para que a abordagem de segurança da informação seja efetiva, o gerenciamento de gestão de riscos de segurança da informação está interligado à outros processos que compõem o Sistema de Gestão de Segurança da Informação (SGSI-IFTO). A figura 3 apresenta estes processos.

Figura 3 - Processos que compõem o SGSI-IFTO

8. PRÁTICAS RECOMENDADAS

A implementação dessas boas práticas é essencial para fortalecer a postura de segurança da informação de uma organização e para enfrentar os desafios constantes de ameaças cibernéticas em evolução. Neste sentido são apresentadas as seguintes práticas para a segurança da informação no IFTO.

1. O processo de gestão de riscos de segurança da informação deve ser alinhado com o modelo de gestão de riscos institucional, compatível com a missão e os objetivos estratégicos do IFTO, processos internos institucionais, requisitos legais, políticas e estrutura organizacional do IFTO.

2. O processo de gestão de riscos de segurança da informação deve fornecer ao IFTO, um plano de gestão de riscos de segurança da informação, relatório de identificação, análise, avaliação e tratamento dos riscos de segurança da informação.

3. O plano de gestão de riscos de segurança da informação deve ser regularmente revisado, a fim de manter atualizados os riscos relativos aos ativos de informação.

4. O processo de implementação do plano de gestão de riscos de segurança da informação deve considerar dentre outros aspectos, as recomendações de mudanças em relação aos critérios de aceitação de riscos, a abrangência da atuação do plano, as ações de segurança da informação e as atividades de tratamento de riscos previstas.

5. O relatório de identificação, análise, avaliação e tratamento dos riscos de segurança de segurança da informação deve ser atualizado anualmente e sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo, devendo ser posteriormente enviado ao gestor de segurança da informação para aprovação.

6. Os ativos de informação devem ser identificados e classificados de forma a permitir avaliar as ameaças potenciais e as vulnerabilidades que podem afetar esses ativos.

7. Sempre que possível deve ser realizada uma análise detalhada dos riscos para avaliar a probabilidade e o impacto dos riscos identificados. Isso ajuda a priorizar ações de mitigação.

8. O IFTO deve desenvolver e implementar controles de segurança adequados para reduzir, mitigar ou eliminar os riscos identificados. Isso pode incluir controles técnicos, administrativos e físicos.

9. O IFTO deve desenvolver e testar planos de resposta a incidentes para lidar rapidamente com incidentes de segurança quando ocorrerem, minimizando os danos e interrupções.

10. O IFTO deve implementar processos contínuos de monitoramento e revisão dos riscos de segurança para identificar novas ameaças, atualizar controles e garantir conformidade contínua.

11. O IFTO deve educar e treinar regularmente os usuários sobre práticas de segurança, garantindo que estejam cientes das políticas e dos procedimentos de segurança.

12. O IFTO deve manter políticas de segurança atualizadas e revisadas regularmente, garantindo que estejam alinhadas com os riscos atuais e as melhores práticas de segurança.

13. O IFTO deve realizar testes regulares de vulnerabilidade e testes de penetração para identificar e corrigir vulnerabilidades nos sistemas e na infraestrutura.

14. O IFTO deve colaborar com outras organizações, compartilhando informações sobre ameaças e práticas de segurança para fortalecer as defesas.

15. O IFTO deve promover uma cultura organizacional focada em segurança da informação, incentivando a responsabilidade individual e o engajamento de todos os colaboradores.

9. **REFERÊNCIAS**

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação. Técnicas de segurança. **NBR ISO/IEC 27005:2019. Gestão de riscos de segurança da Informação.**

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Controladoria-Geral da União. **Instrução Normativa Conjunta nº 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.** Brasília, DF: Presidência da República, 2016. (2016a). Disponível em: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content /id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. Acesso em: 26 set 2022.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação. **Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal.** Brasília, DF: Ministério do Planejamento, Desenvolvimento e Gestão, ago. 2016. (2016b). Disponível em: https://www.gov.br/governodigital/pt-br/sisp/mgr-sisp-v260816.pdf/view. Acesso em: 10 mai. 2020.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicação. **Metodologia de gestão de segurança da informação e comunicações**. Disponível em: https://datasus.saude.gov.br/wp-content /uploads/2019/08/Norma-Complementar-n%C2%BA-02IN01DSICGSIPR.pdf. Acesso em: 21 set. 2022.

BRASIL. Presidência da república. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Gestão de riscos de segurança da informação e comunicações. Norma complementar 04 de 15 de fevereiro de 2013**. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-04IN01DSICGSIPR.pdf. Acesso em: 21 set. 2022.

BRASIL. Controladoria-Geral da União. **Metodologia de Gestão de Riscos da CGU, versão 2.0. Brasília, DF: Controladoria-Geral da União. 2021.** Disponível em: https://repositorio.cgu.gov.br/bitstream /1/65535/6/Metodologia_de_riscos_2_0.pdf. Acesso em: 26 set. 2022.

ESCOLA SUPERIOR DE REDES. **Como fazer gestão de riscos de segurança da informação na empresa?** Brasília-DF. Rede Nacional de Pesquisa, 2022. Disponível em: https://esr.rnp.br/governanca-de-ti/gestao-de-riscos-da-seguranca-da-informacao/. Acesso em: 13 fev. 2022.

FERNANDES, Jorge Henrique Cabral. **Introdução à gestão de riscos de segurança da informação.** CEGSIC 2009-2011. Disponível em: https://www.trf3.jus.br/documentos/rget/seguranca /CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf. Acesso em: 13 fev. 2022.

HM Government (HMG). ***The Orange Book: Management of Risk Principles and Concepts.*** 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system /uploads/attachment_data/file/866117 /6.6266_HMT_Orange_Book_Update_v6_WEB.PDF. Acesso em: 11 jun. 2020.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS. **Gestão de riscos – IFTO: metodologia de implantação.** Palmas: IFTO, 2015. Disponível em: http://www.ifto.edu.br/ifto/reitoria /diretoria-sistemica/infraestrutura/documentos-de-referencia/gestao-de-riscos-metodologia-do-ifto/view. Acesso em: 10 jun. 2020.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ***31000: 2018: Risk management: guidelines, provides principles, framework and a process for managing risk.*** 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ***31010:2019: Risk Management: Risk assessment techniques.*** 2019.

PROJECT MANAGEMENT INSTITUTE (PMI). **A Guide to the Project Management Body of Knowledge.** Project Management Institute. 5. ed. Pennsylvania, USA, 2013.

TRIBUNAL DE CONTAS DA UNIÃO. **Manual de Gestão de Riscos do TCU.** 2ª ed. Brasília, DF: TCU, 2020. Disponível em: https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/. Acesso em: 26 set. 2022.

TRIBUNAL DE CONTAS DA UNIÃO. **Referencial Básico de Gestão de Riscos. SEGECEX/COGER.** Brasília, DF: TCU, 2018b. Disponível em: https://portal.tcu.gov.br/data/files/21/96/61/6E /05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf. Acesso em: 10 jun. 2020.

TRIBUNAL DE CONTAS DA UNIÃO. **Gestão de riscos: avaliação da maturidade.** Brasília, DF: TCU, 2018c. Disponível em: https://portal.tcu.gov.br/data/files/0F/A3/1D/0E /64A1F6107AD96FE6F18818A8/Gestao_riscos_avaliacao_maturidade.pdf. Acesso em: 10 jun. 2020.

ANEXO I

Ativos de informação que serão objetos do processo de gestão de riscos de segurança da informação

Ativo (Sistema de Informação)	Descrição	Responsável	Processo de Negócio Relacionados
Moodle	Ambiente Virtual de Aprendizagem	PROEN PROEX	- Gestão de Cursos de Ensino - Gestão de Cursos de Extensão
SEI	Sistema Eletrônico de Informações	Chefia de gabinete	- Processo Eletrônico de Documentos
SI	Sistemas Internos	PROEX PROEX DGP	- Gestão de restaurantes - Agendamento do e-kids - Gestão de eventos institucionais
SOPHIA	Sistema de Gestão de Bibliotecas	Bibliotecas	- Gestão de Bibliotecas
SUAP	Sistema Unificado de Administração Pública	PROEN PROAD PROEX PROAE	- Gestão administrativa. - Gestão acadêmica. - Ensino. - Pesquisa. - Extensão. - Frotas. - Patrimônio. - Contratos.
Portal Institucional	Site Oficial	DICOM	- Gestão de conteúdos institucionais.

ANEXO II

Plano de Gestão de Riscos de Segurança da Informação

Identificação			Análise/Avaliação				Tratamento	
Ameaça	**Tipo**	**Fonte**	**Causa**	**Consequência**	**Probabilidade**	**Impacto**	**Controle**	**Responsável**
Furto de equipamento.	Imagem Financeiro	Pessoas	- Inexistência de mecanismos de proteção física no prédio, portas e janelas.	-Indisponibilidade de equipamento para realização de atividades setoriais.	média	médio	- Política de segurança da informação. - Segurança física e do ambiente. - Processo de controle de acesso à informação e aos ativos associados à informação.	Patrimônio
Destruição de equipamento.	Imagem Financeiro	Infraestrutura	- Mau uso do equipamento. - Vandalismo.	-Indisponibilidade de equipamento para realização de atividades setoriais.	média	médio	- Política de segurança da informação. - Segurança física e do ambiente. - Processo de controle de acesso à informação e aos ativos associados à informação.	Patrimônio
Ataques cibernéticos (ransomware, phishing, DNS cache poisoning, malware entre outros).	Operacional Imagem	Externa	-Falha humana relacionada a configuração das regras de segurança dos Sistemas de detecção de intrusos HIDS/NIDS. -Desatualização de sistemas operacionais e softwares. -Vulnerabilidades ou erros de configuração em equipamentos, serviços e sistemas operacionais.	-Roubo de informações armazenadas em computadores, servidores ou outros dispositivos com a intenção de comprometer a privacidade ou obter/divulgar informações confidenciais. -Vazamento de informações críticas como senhas de sites com autenticação, como redes sociais, painéis administrativos, e-mails, etc. -Comprometimento da imagem institucional. Perda de dados. -Indisponibilidade de serviços, recursos e sistemas informatizados.	média	alto	- Política de segurança da informação. - Gestão de incidentes de segurança da informação.	Diretoria de Tecnologia da Informação
Oscilações na comunicação entre os campus envolvendo links de internet e VPN.	Operacional	Infraestrutura	- Falha humana relaciona a configurações incorretas dos firewalls. - Erros de	- Indisponibilidade de rede de comunicação de dados.	média	alto	- Processo de gestão de continuidade de serviços de Tecnologia da Informação.	Diretoria de Tecnologia da Informação

			hardware. - Queima de componentes eletrônicos. - Quedas de link devido rompimento de fibra óptica decorrente de execução de obras públicas, desastres ou acidentes. - Queda de link em razão o mal funcionamento de componentes eletrônicos. -Configuração incorreta de roteador ou firewall.				- Processo de gestão de incidentes de segurança da informação.	
Indisponibilidade de links de comunicação de dados.	Operacional	Infraestrutura	- Falha humana relaciona a configurações incorretas dos firewalls. - Erros de hardware. - Queima de componentes eletrônicos. - Quedas de link devido rompimento de fibra óptica decorrente de execução de obras públicas, desastres ou acidentes. - Queda de link em razão o mal funcionamento de componentes eletrônicos. -Configuração incorreta de roteador ou firewall.	- Indisponibilidade de rede de comunicação de dados.	média	alto	- Processo de gestão de continuidade de serviços de tecnologia da informação. - Processo de gestão de incidentes de segurança da informação.	Diretoria de Tecnologia da Informação
Abuso de direitos de acesso.	Operacional Imagem	Processo	- Erros de configuração de mecanismos de controle de acesso a dados. - Inexistência de política de atualização de sistemas.	- Perda de dados institucionais.	média	alto	- Política de segurança da informação. - Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Espionagem.	Operacional Imagem Legal	Externa	- Arquitetura insegura da rede. - Falhas no mecanismo de armazenamento de senhas.	- Perda de dados institucionais.	média	alto	- Política de segurança da informação. - Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Acesso não autorizado a sistemas de informação, recursos e serviços de TI.	Operacional Imagem Legal	Processo	- Falha operacional no controle de permissões.	- Acesso indevido (permissões indevidas) a um ambiente físico ou lógico. - Vazamento de informações. - Comprometimento de dados.	média	alto	- Política de segurança da informação. - Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Coleta excessiva de dados em sistemas de informação, recursos e serviços de TI.	Operacional Imagem Legal	Processo	- Falha operacional na coleta de dados.	- Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.	média	alto	- Política de privacidade. - Processo de Software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Compartilhamento de dados pessoais com terceiros sem autorização do usuário.	Operacional Imagem Legal	Processo	- Falha operacional no tratamento de dados.	- Instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais (LGPD, art. 27).	média	alto	- Política de privacidade. - Processo de Software. -Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Falha em considerar os direitos do titular dos dados pessoais (perda do direito de acesso).	Operacional Imagem Legal	Processo	- Falha operacional no tratamento de dados.	- Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 23 da LGPD. Art. 17. O titular dos dados pessoais tem direito a obter do controlador mediante requisição: I - Confirmação da existência de tratamento; II - Acesso aos dados; III - Correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados	média	alto	- Política de privacidade. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação

				desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5o do art. 8 desta Lei.				
Processamento ilegal de dados.	Operacional Imagem Legal	Processo	- Inexistência de mecanismos de monitoramento de alteração de dados.	- Comprometimento de dados.	média	alto	- Sistema de Gestão de Segurança da Informação. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Informação insuficiente sobre a finalidade do tratamento de dados pessoais.	Operacional Imagem Legal	Processo	- Falha operacional no tratamento de dados.	- O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma transparente e clara ao detentor dos dados pessoais.	baixa	médio	- Política de privacidade. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Modificação de dados não autorizada nos sistemas de informação, recursos e serviços de TI.	Operacional Imagem Legal	Pessoas	- Falha operacional no tratamento de dados.	- Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.	média	alto	- Sistema de gestão de segurança da informação. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Reidentificação de dados pseudonimizados.	Operacional Imagem Legal	Processo	- Falha operacional no tratamento de dados.	- Dados pessoais podem ser reidentificados por cruzamento simples de dados pessoais (LGPD, art. 12 e 13).	média	alto	- Política de privacidade. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Retenção prolongada de dados pessoais sem necessidade nos sistemas operacionais, recursos e serviços de TI.	Operacional Imagem Legal	Processo	- Falha operacional no tratamento de dados.	- Uso indevido de dados pessoais.	média	alto	- Política de privacidade. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Roubo de dados armazenados nos sistemas de informação, recursos e serviços de TI.	Operacional Imagem Legal	Pessoas Processo Externa	- Falha operacional no processo de proteção de dados.	- Uso indevido de dados institucionais.	média	alto	- Sistema de gestão de segurança da informação. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Tratamento de dados sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente).	Operacional Imagem Legal	Processo	- Falha operacional no tratamento de dados.	- Controlador de dados pessoais não obtém consentimento do titular para realizar um tratamento de dados pessoais sem embasamento legal.	média	alto	- Política de privacidade. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	Operacional Imagem Legal	Pessoas Processo	- Falha do tratamento de dados.	- A realização de operação de processamento de dados pessoais deve estar em conformidade com a LGPD. Qualquer operação de processamento que não atenda esse	média	alto	- Política de privacidade. - Processo de software. - Processo de controle de acesso à informação e aos ativos associados à	Diretoria de Tecnologia da Informação

				requisito pode produzir informações com vinculações ou associações indevidas.			informação.	
Uso não autorizado de equipamento.	Operacional Imagem Legal	Processo	- Erros de configuração de mecanismos de controle de acesso a dados. - Inexistência de política de controle de acesso.	- Perda de dados e informações institucionais. - Roubo de informações.	média	média	- Política de segurança da informação. - Sistema de gestão de segurança da informação. - Processo de Gestão de ativos. - Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Dados corrompidos em razão de diversas situações.	Operacional Imagem Legal	Processo	- Quedas ou oscilações de energia. - Queima de componentes eletrônicos. - Erro de software. - Erros de rede. - Erros de Configuração das estratégias de Backups.	- Perda de dados e informações institucionais. - Roubo de informações.	média	muito alto	- Política de backup e restauração de dados. - Processo de gestão de continuidade de serviços de TI.	Diretoria de Tecnologia da Informação
Uso de cópias de software falsificadas ou ilegais.	Operacional Imagem Legal	Processo	- Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual.	- Violação de direitos autorais. - Ataques cibernéticos. - Roubo de informações. - Sequestro de informações. - Adulteração de informação.	média	média	- Política de segurança da informação. - Sistema de gestão de segurança da informação. - Inventário de software. - Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Comprometimento de dados.	Operacional Imagem Legal	Processo	- Erros de configuração de mecanismos de controle de acesso a dados. - Inexistência de política de atualização de sistemas.	- Perda de dados	média	média	- Política de segurança da informação. - Política de padronização e atualização tecnológica. - Controle de acesso. - Política de backup e restauração de dados. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Variação de temperaturas na sala de Equipamentos (Datacenter).	Operacional	Processo	-Defeitos em componentes eletrônicos dos aparelhos de ar condicionado.	-Superaquecimentos dos ativos. - Danos pontuais aos equipamentos, podendo causar defeitos ao longo do tempo de vida do equipamento. -Queima de componentes. eletrônicos -Indisponibilidade recursos, serviços e sistemas informatizados.	média	médio	-Sistema redundante de climatização de salas. -Gestão de continuidade de serviços de TI. Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Ataques internos aos recursos computacionais.	Operacional Imagem	Pessoas	-Ausência de sistema de monitoramento de vulnerabilidades. -Ausência de mecanismos de proteção contra invasão. -Ausência de sistema de detecção de intrusão. -Ausência de norma sobre controle de acesso à rede. -Ausência de -Política de Segurança da Informação. -Dano ao Datacenter.	-Roubo ou perda de informações. Indisponibilidade recursos, serviços e sistemas informatizados.	alta	alto	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Quantidade insuficiente de especialistas em segurança da informação para sanar vulnerabilidades em sistemas de informação, recursos e serviços de TI.	Operacional	Pessoas	-Ausência de capacitações na área de segurança da informação.	-Indisponibilidade de serviços, recursos e sistemas informatizados. -Perda de dados. -Roubo de informações.	alta	alto	-Plano Anual de Capacitações. -Segurança em recursos humanos.	Diretoria de Tecnologia da Informação
Falhas no acesso aos dados armazenados no banco de dados.	Operacional Imagem Legal	Infraestrutura	-Inexistência de conectividade de rede. -Falhas ou erros na configuração do serviço.	-Indisponibilidade de recursos, serviços e sistemas informatizados. -Perda de dados. -Roubo de	alta	alto	- Processo de controle de acesso à informação e aos ativos associados à	Diretoria de Tecnologia da Informação

			-Comprometimento do sistema operacional. -Ataques internos e externos.	informações.			informação	
Falhas de conexão com a rede lógica de dados.	Operacional Imagem Legal	Infraestrutura	-Erros de configuração de ativos de rede. -Quedas ou oscilações de energia. -Queima ou falhas de componentes eletrônicos dos ativos de rede. -Falta de conhecimento sobre cabeamento estruturado. -Ausência de capacitações em redes de comunicação de dados. -Falha humana.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	alta	alto	- Processo de gestão de continuidade de serviços de Tecnologia da Informação. - Processo de controle de acesso à informação e aos ativos associados à informação	Diretoria de Tecnologia da Informação
Falhas de validação de credenciais no sistema de autenticação do usuário.	Operacional Imagem Legal	Processo	-Falhas em componentes eletrônicos. -Falha humana.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	alta	alto	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Interrupções no acesso dos dados armazenados no storage de dados.	Operacional	Infraestrutura	-Falhas na comunicação de dados. -Oscilações de energia elétrica. -Procedimento incorreto de acesso ao *storage*. -Procedimento incorreto de configuração do *storage*.	-Indisponibilidade de recursos, serviços e sistemas informatizados.	alta	alto	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Remoção não autorizada de dados institucionais nos sistemas de informação de forma que compromete a execução de processo organizacionais.	Operacional	Infraestrutura	- Falha operacional na configuração de permissão de acesso de usuários.	- Falta de informação importante para execução de processo organizacional.	média	médio	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Perda de dados em razão de erros operacionais de usuários.	Operacional	Processo	- Falhas nos mecanismos de controle de acesso.	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
E-mails e websites de phishing que roubam dados confidenciais e senhas.	Operacional	Processo	- Falhas nos IDS e IPS.	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Processo de gerenciamento de incidentes de segurança da informação.	Diretoria de Tecnologia da Informação
Golpes de engenharia social, que usam a manipulação para persuadir pessoas e roubar informações privadas.	Operacional	Processo	- Falhas nos mecanismos de controle de acesso às informações.	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Programa de conscientização e treinamento em segurança da informação	Diretoria de Tecnologia da Informação
Ações de sabotagem que bloqueiam o acesso aos dados e recursos do sistema, como os ataques de negação de serviço (ataques DoS e DDoS).	Operacional	Processo	- Falhas nos IDS e IPS.	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Invasão e roubo de dispositivos móveis que armazenam informações críticas, como smartphones, tablets e wearables.	Operacional	Processo	- Falhas nos mecanismos de controle de acesso aos ativos de informação.	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Vazamento de dados por falhas internas ou ataques externos.	Operacional Imagem Legal	Processo	- Falhas nos mecanismos de controle de acesso aos ativos de informação.	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Extorsão e sequestro de informações, como no caso dos malwares, que bloqueiam o acesso aos dados e exigem um resgate para liberá-los.	Operacional Imagem Legal	Processo	- Falhas nos mecanismos de controle de acesso aos ativos de informação.	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Processo de controle de acesso à informação e aos ativos associados à informação.	Diretoria de Tecnologia da Informação
Perda de dados por falhas de hardware ou software.	Operacional	Infraestrutura	- Queima de componentes eletrônicos. - Oscilações elétricas	-Indisponibilidade de informações para execução do processo organizacional.	média	médio	- Processo de gestão de continuidade de serviços de Tecnologia da Informação.	Diretoria de Tecnologia da Informação
Intercepção de informações por terceiros não autorizados.	Operacional Imagem	Processo	- Falhas nos procedimentos e soluções de gestão de segurança da informação	-Roubo de dados e informações.	média	médio	Prática de segurança da informação	Diretoria de Tecnologia da Informação

Negligência de usuário no manuseio de informações.	Operacional	Processo	- Falha humana	-Roubo de dados e informações	média	médio	Programa de conscientização e treinamento em segurança da informação	Diretoria de Tecnologia da Informação

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 05/01/2024, às 19:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2218393** e o código CRC **63AE5751**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.ifto.edu.br — reitoria@ifto.edu.br